ОСОБЕННОСТИ ПРЕДЛОЖЕННОГО ПОДХОДА

К недостаткам решения, предложенного в данной работе, следует отнести недостатки, присущие статистическим методам вообще. Некоторые незначительные изменения в состоянии сетевого трафика, например сканирование портов с очень малой скоростью, может быть незамеченным.

ЗАКЛЮЧЕНИЕ

В данной работе исследован статистический метод анализа сетевого трафика, определены его преимущества и недостатки в сравнении с сигнатурным методом анализа, создан программный комплекс, способный анализировать и обнаруживать нехарактерную для сети активность, тем самым, пресекая атаки, неизвестные для сигнатурных средств защиты. Дальнейшим развитием статистического метода может быть его способность самообучаться и сохранять результаты своих анализов.

Литература

1. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2003.
2. *Хогдал Дж. Скотт.* Анализ и диагностика компьютерных сетей. Addison Wesley Longman, Inc., 2000.
3. *Юдицкий С. С., Швецов В .И.* Увидеть слона целиком // Сети и системы связи. 2001. № 10.
4. *Айвазян С. А., Енюков И. С., Мешалкин Л. Д.* Прикладная статистика: Исследование зависимостей. М.: Финансы и статистика, 1985. 488 с.

ЗАЩИТА ИНФОРМАЦИИ ОТ КОПИРОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ СМЕННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

А. С. Кудин

Эффективная борьба с пиратством в области IT-технологий в настоящее время является актуальной задачей. Существует несколько методов борьбы с пиратством, например: легитимный (взлом и незаконное распространение программного обеспечения описаны в законах и строго преследуются по ним), экономический (цена товара делается сравнимой с ценой подделки). Часто наиболее эффективной является техническая защита программных продуктов от копирования.

Защиту программного обеспечения, распространяемого на сменном носителе информации, надежнее всего построить на проверке уникальности этого носителя. В настоящее время подавляющее большинство ПО распространяется на CD и DVD дисках, поэтому о них и пойдет речь далее.

Целью данной работы было создание ПО для записи и защиты CD дисков с документами. Защита должна допускать просмотр документов только с оригинального диска и пресекать их прямое копирование. Платформой для создаваемого ПО была выбрана ОС Windows.

Реализация поставленной цели предполагает решение трех задач:

- проверка CD диска на подлинность,
- шифрование/расшифровка документов с CD диска,
- реализация модулей для просмотра документов пользователем.

Оригинальный диск должен иметь уникальную некопируемую метку, наличие которой можно проверить на оборудовании конечного пользователя. Разработчиками защит придумано много различных способов пометки дисков. Вот некоторые из них:

- Искажение TOC (Table Of Contents),
- Искажение нумерации треков и секторов,
- Неустойчивые и ошибочные секторы,
- Измерение временных характеристик чтения секторов,
- Измерения углов между секторами.

Последние два метода наиболее предпочтительны, так как не нарушают существующие стандарты записи дисков и не требуют использования специального оборудования (защищенный диск может быть записан обычным пишущим приводом).

В нашей реализации защиты был использован метод измерения углов между секторами. Он работает следующим образом. Производится чтение нескольких секторов с убывающими LBA (Logical Base Address) адресами (т.е. сектора читаются в направлении к центру диска). Пусть сектор *y* читается после сектора x (*рис. 1*). Если y расположен как показано на *рис. 1а*, т.е. после сектора *x* в направлении вращения диска, то читающей диску надо лишь немного повернуться – и читающая головка будет над сектором *y*, т.е. время чтения его будет небольшим. Если же секторы расположены как показано на *рис. 1б*, то диск совершит почти полный оборот, прежде чем сектор *y* будет прочитан, поэтому время чтения будет большим.

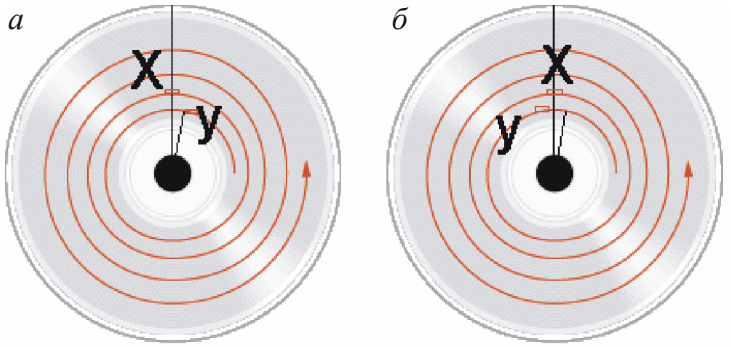

Рис 1. Взаимное расположение последовательно читаемых секторов на диске

Таким образом, после чтения диска

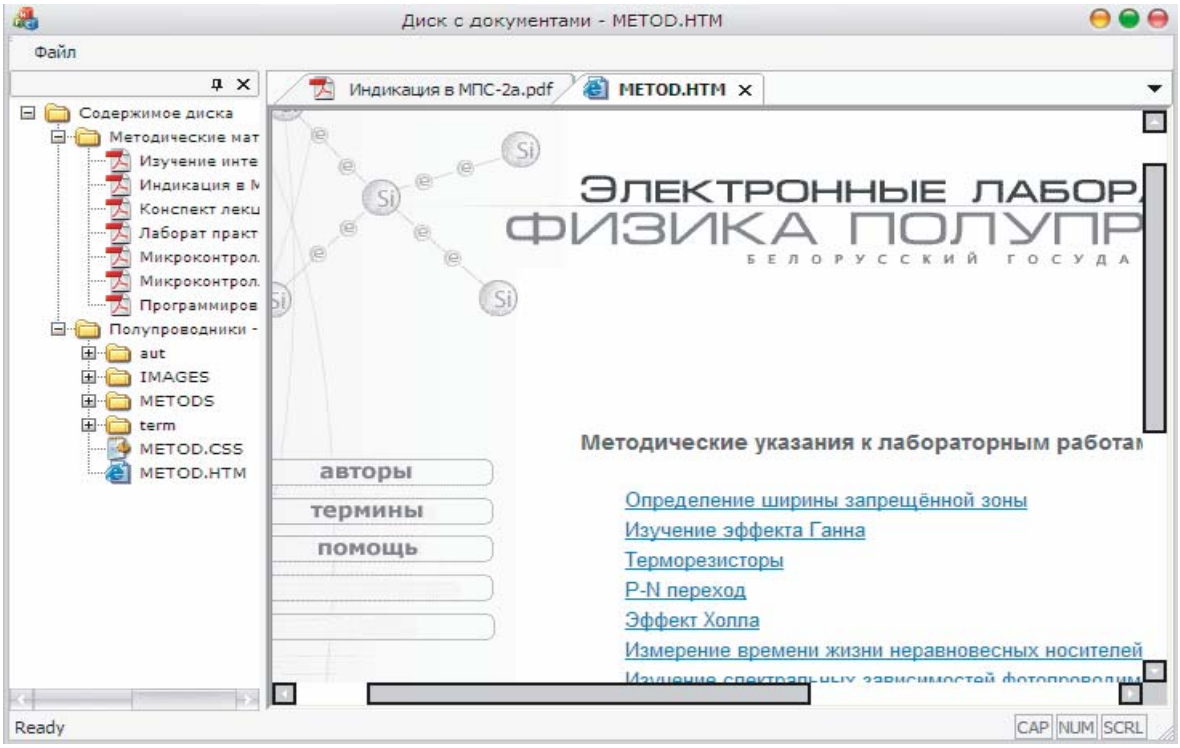

Рис 2. Просмотр содержимого диска в программе-оболочке

будет получена последовательность чисел – времен чтения секторов, которая существенно различается у разных дисков. Поэтому ее можно будет использовать для проверки диска на подлинность и расшифровки документов.

В нашей версии защиты зашифрованные документы записываются в специальный файл на диске, причем древовидная структура папок сохраняется. В качестве алгоритма шифрования документов используется побайтовая операция XOR с ключом, сгенерированным на основе последовательности времен чтения. Т.к. при использовании одинакового ключа для всех документов надежность шифрования падает, значение ключа также зависит от размера шифруемого файла.

Проверку диска на подлинность и отображение документов выполняет программа-оболочка, запускаемая автоматически с диска после его загрузки в привод. Программа-оболочка (рис. 2) написана в среде разработки Microsoft Visual Studio с использованием библиотеки классов MFC.

В нашей версии защиты была реализована возможность просмотра HTML страниц и PDF документов. HTML страницы показываются через ядро Internet Explorer – ActiveX элемент «Microsoft Web Browser», который присутствует во всех версиях ОС Windows. Так как зашифрованные файлы организуются в древовидную структуру, HTML страницы могут

содержать ссылки на внешние фалы, то есть картинки, определения стилей и так далее. Просмотр PDF документов осуществляется с использованием кроссплатформенной библиотеки с открытым исходным кодом Poppler.

Процесс записи защищенного диска состоит из следующих шагов:

- Запись программы-оболочки и всех необходимых ей библиотек первой сессией на диск;
- Измерение углов между секторами записанной сессии;
- Шифрование защищаемых документов и запись их в виде одного файла на диск во второй сессии;
- Запись специального файла с данными корректировки погрешностей измерения углов между секторами во второй сессии. Данные в этом файле позволяют получать одно и то же значение ключа для расшифровки документов при неизбежных небольших погрешностях в измерении углов.

Литература

1. *Касперски К.* Техника защиты компакт-дисков от копирования. БХВ-Петербург, 2004. ISBN: 5-94157-412-6 978-5-94157-412-4
2. Интернет-адрес: http://www.insidepro.com/rus/doc,
   Интернет-адрес: http://msdn.microsoft.com/
3. Интернет-адрес: http://poppler.freedesktop.org/
4. Интернет-адрес: http://www.nero.com/enu/downloads-sdk.html
5. Интернет-адрес:
   http://www.ecma-international.org/publications/standards/Ecma-130.htm

ПОСТРОЕНИЕ И ОПТИМИЗАЦИЯ ПОЛЯ НАПРАВЛЕНИЙ ПАПИЛЛЯРНЫХ ЛИНИЙ ДАКТИЛОСКОПИЧЕСКИХ ИЗОБРАЖЕНИЙ В СИСТЕМАХ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

А. В. Кудько

Прежде, чем дактилоскопическое изображение, полученное со сканера, будет опознано, а сам отпечаток проанализирован и распознан, необходимо провести его обработку. Одним из вариантов классификации и анализа дактилоскопического изображения является его обработка с помощью полей направлений и выделение на основе этих полей особенностей структур отпечатков. К достоинствам полей направлений относится их достаточная нечувствительность к помехам, полученным при сканировании отпечатка и изменении линий в процессе сканирования. К недостаткам стоит отнести чувствительность полей направлений к повороту изображения при сканировании.